Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ FÉLIX HOUPHOUËT-BOIGNY

UFR DE MATHEMATIQUES ET INFORMATIQUE

RÉPUBLIQUE DE CÔTE D'IVOIRE

Union – Discipline - Travail

Année Universitaire 2025 – 2026

Licence 3 – Réseaux Informatique Sécurité et Télécommunications

VIRTUALISATION ET SUPERVISION DES RESEAUX

centreon

Produit par :

AGBENONZAN Kossivi Jacques Junior

Encadreur : Dr Medard KOUASSI

VIRTUALISATION ET SUPERVISION DES RESEAUX

Nom et Prénoms : AGBENONZAN Kossivi Jacques Junior

Encadreur : Dr Medard KOUASSI

Année Universitaire : 2025-2026

Introduction

Dans le cadre des travaux pratiques portant sur la virtualisation et la supervision des réseaux, ce document présente la mise en œuvre d'une solution complète de supervision. L'objectif est de démontrer, étape par étape, la méthodologie adoptée pour installer, configurer et intégrer différents serveurs (Linux, Windows) au sein d'une plateforme centralisée.

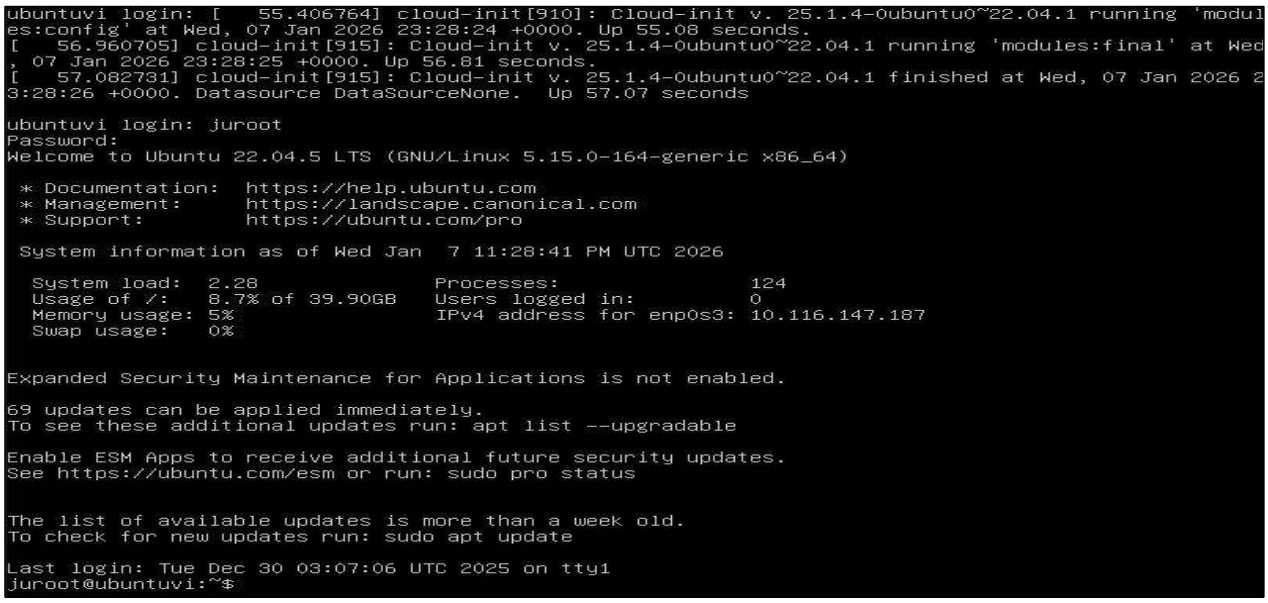
La solution retenue repose sur Centreon, déployé dans un environnement virtualisé grâce à **VMware Workstation Pro**. Ce choix permet de reproduire un contexte réaliste tout en offrant la flexibilité nécessaire pour tester et valider les fonctionnalités de supervision.

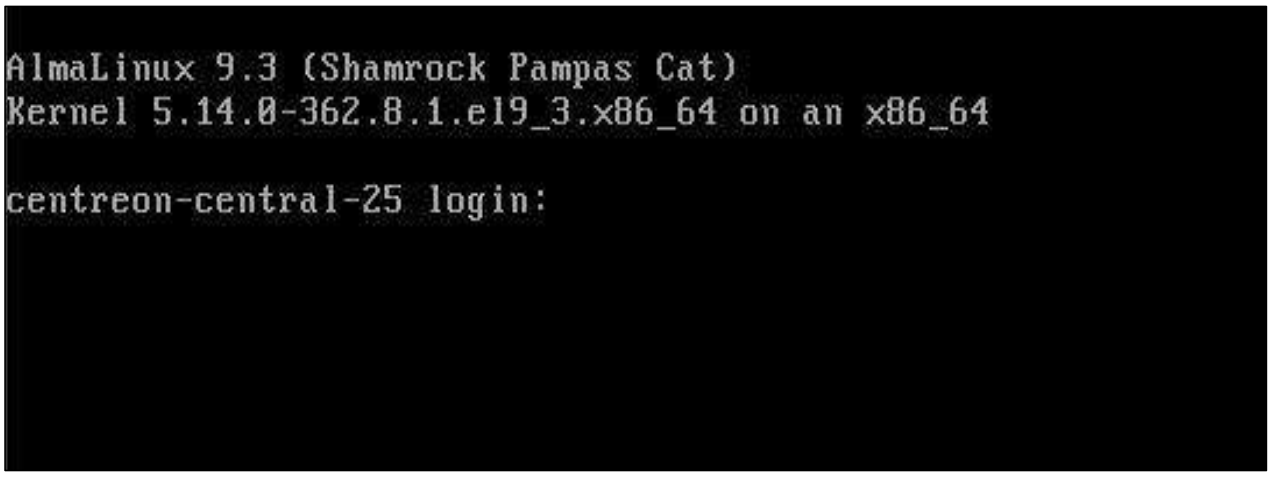
Au-delà de l'installation technique, ce travail met en évidence :

- ✓ L'importance de l'adressage réseau et de la configuration SNMP,
- ✓ la création et l'intégration des hôtes et services supervisés,
- ✓ la mise en place des notifications pour garantir une réactivité optimale, ainsi que la réalisation de scénarios de tests validant le bon fonctionnement du système.

Ce projet illustre concrètement comment une organisation peut assurer la fiabilité, la disponibilité et la sécurité de son infrastructure grâce à une supervision centralisée et automatisée, tout en offrant une visibilité accrue sur l'état des ressources et des services critiques.

1. Etape 1 Virtualisation





2. Etape 2 : Connexion au serveur CENTREON

À cette étape, l'administrateur renseigne son identifiant **root** ainsi que le mot de passe **Centreon** afin de s'authentifier. Une fois la connexion validée, il accède au shell Linux, ce qui lui donne la possibilité d'exécuter l'ensemble des commandes indispensables à la gestion et à la configuration du serveur Centreon.

3. Etape 2 : Identification de l'adresse IP de la machine virtuelle

L'adressage réseau représente une étape essentielle pour permettre l'accès distant à la plateforme. L'adresse IP de la machine virtuelle peut être identifiée à l'aide des commandes :

```
“bash’’’
hostname
```

Ou

```
“bash’’’
ip a
```

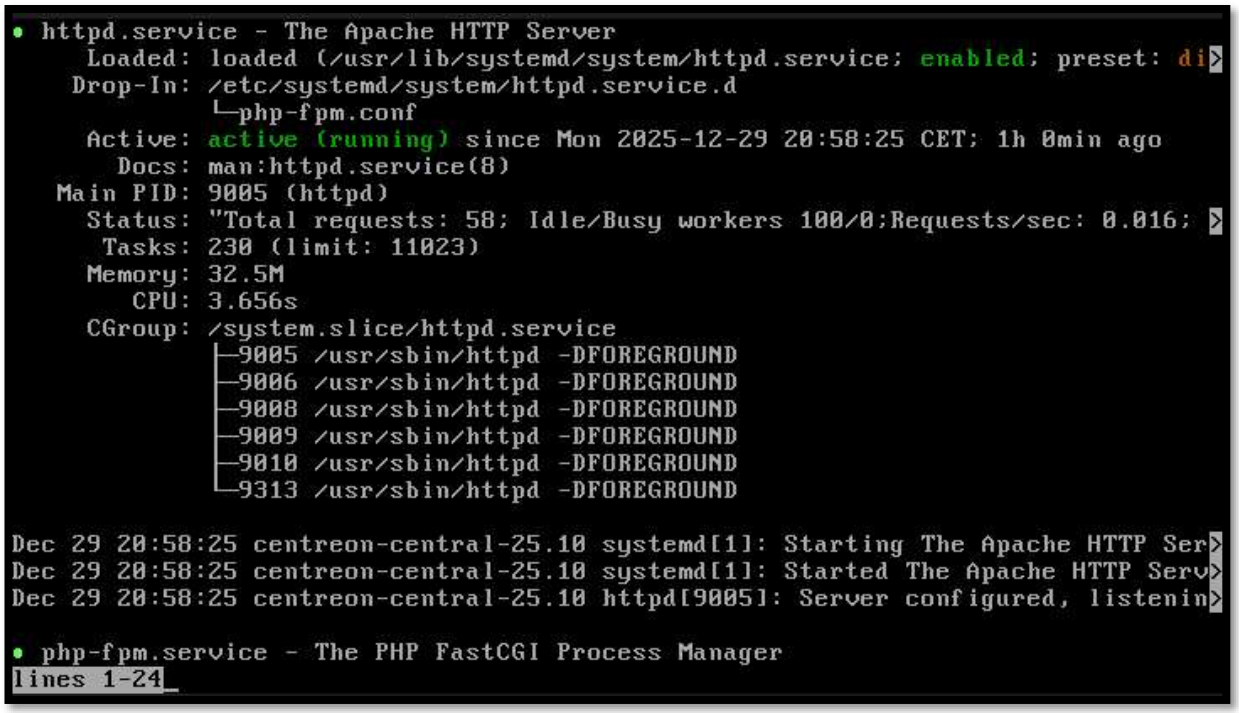
Cette adresse peut être attribuée automatiquement par un serveur DHCP ou définie manuellement, en fonction de la topologie du réseau.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 08:00:27:af:0d:ce brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 172.28.180.185/24 brd 172.28.180.255 scope global dynamic noprefixroute
 eth0
```

4. **Étape 3 : Vérification des services critiques**

Afin de s'assurer que les services critiques sont bien actifs, il convient d'exécuter la commande suivante :

```
"bash"
sudo systemctl status httpd php-fpm mariadb cbd
centengine gorgoned centreontrap
```



Cette vérification permet de confirmer que chaque service nécessaire au bon fonctionnement de Centreon est opérationnel. Un résultat positif à cette vérification atteste que le serveur fonctionne correctement et qu'il est pleinement opérationnel.

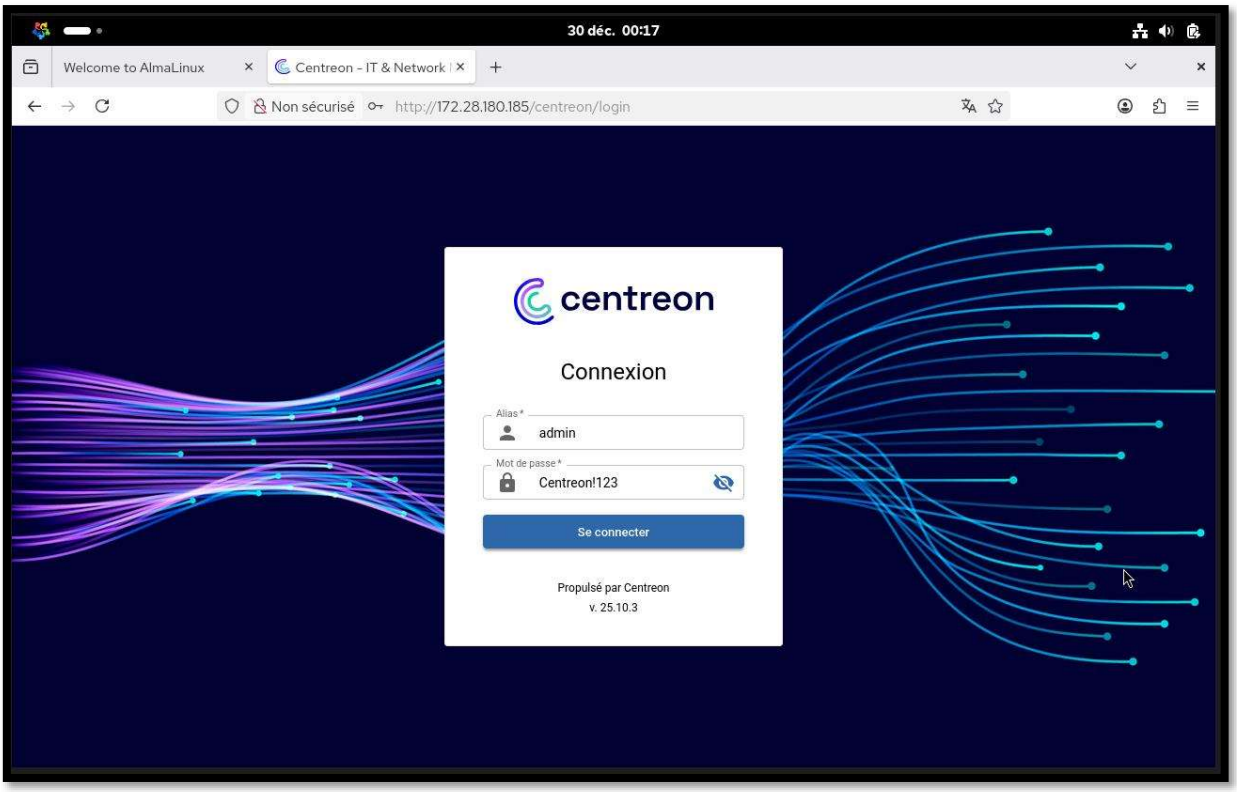
5. **Étape 5: Accès à l'interface web de Centreon**

http://<IP_VM>/Centreon

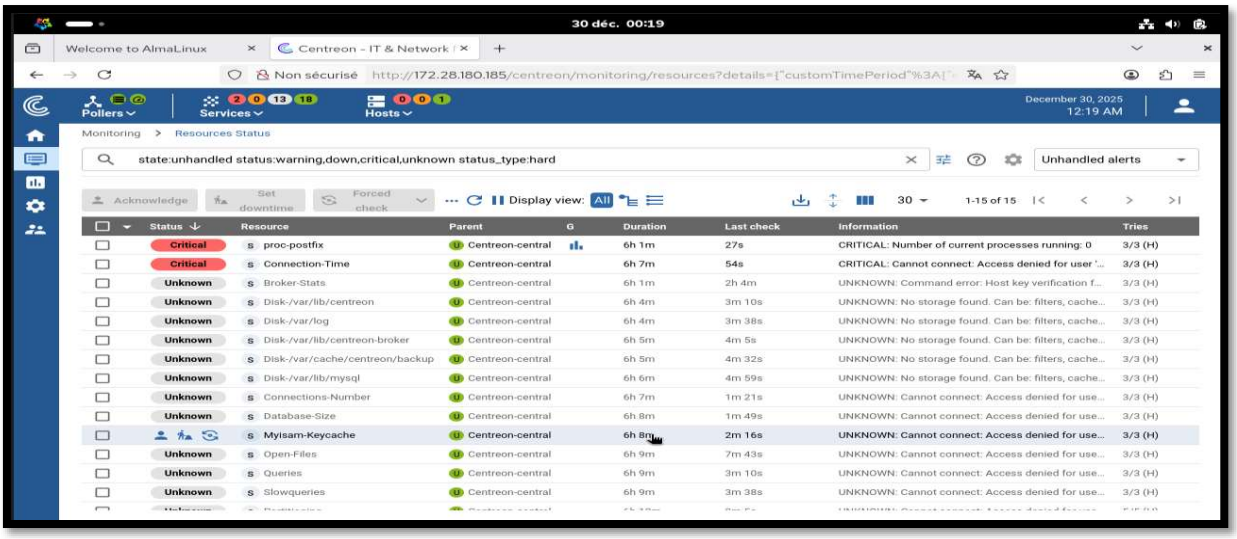
Les identifiants par défaut sont :

- **Nom d'utilisateur** : admin
- **Mot de passe** : Centreon!123

Lors de la première connexion, il est impératif de modifier ce mot de passe afin de sécuriser l'accès à l'interface et d'éviter toute intrusion non autorisée.



Après s'être authentifié sur l'interface web de Centreon, l'utilisateur accède à un tableau de bord initial. Celui-ci présente une vue d'ensemble de l'état global des hôtes ainsi que des services supervisés par défaut. Ce tableau est illustré dans la figure ci-dessous.



L'installation de **Centreon 25.10.0** à partir de l'ISO s'achève avec succès par l'accès à l'interface web. À ce stade, le serveur et la plateforme sont fonctionnels, mais restent encore non opérationnels. Afin de rendre le système pleinement exploitable, il est nécessaire de procéder aux différentes configurations.

II- Configuration

La configuration s'articule autour de trois étapes principales :

- **Installation des paquets nécessaires au service Centreon**
- **Mise en place du service SMTP pour l'envoi des notifications**
- **Intégration des équipements à superviser**

1- **Installation des paquets liées aux services Centreon**

- **Mise à jour du système**

Avant d'entamer toute installation, il est essentiel de mettre à jour le système d'exploitation afin de garantir la stabilité et la compatibilité des bibliothèques requises. Cette opération s'effectue à l'aide de la commande suivante :

```bash
Installing weak dependencies:
 libxcrypt-compat          x86_64 4.4.18-3.el9                appstream      88 k
 rpm-plugin-systemd-inhibit x86_64 4.16.1.3-39.el9            appstream      15 k

Transaction Summary
================================================================================
Install   31 Packages
Upgrade  311 Packages

Total download size: 995 M
Downloading Packages:
(1/342): liburing-2.5-1.el9.x86_64.rpm              62 kB/s |  38 kB     00:00
(2/342): libxcrypt-compat-4.4.18-3.el9.x86_64.r 116 kB/s |  88 kB     00:00
(3/342): mysql-common-8.0.44-1.el9_7.x86_64.rpm 167 kB/s |  67 kB     00:00
(4/342): mysql-selinux-1.0.14-1.el9_6.noarch.rp 186 kB/s |  36 kB     00:00
(5/342): checkpolicy-3.6-1.el9.x86_64.rpm       263 kB/s | 351 kB     00:01
(6/342): policycoreutils-python-utils-3.6-3.el9 316 kB/s |  70 kB     00:00
(7/342): python3-audit-3.1.5-7.el9.x86_64.rpm   332 kB/s |  83 kB     00:00
(8/342): python3-distro-1.5.0-7.el9.noarch.rpm  205 kB/s |  36 kB     00:00
(9/342): python3-libsemanage-3.6-5.el9_6.x86_64 333 kB/s |  78 kB     00:00
```

- **Installation des paquets**

L’installation des paquets indispensables au fonctionnement de Centreon s’effectue en exécutant la commande suivante :

```bash
[root@centreon-central-25 ~]# sudo yum install centreon
Last metadata expiration check: 2:50:14 ago on Mon 29 Dec 2025 06:06:37 PM CET.
Package centreon-25.10.0-1.el9.noarch is already installed.
Dependencies resolved.
================================================================================
 Package           Arch    Version          Repository                     Size
================================================================================
Upgrading:
 centreon          noarch  25.10.3-1.el9    centreon-25.10-stable-noarch  3.1 k
 centreon-central  noarch  25.10.3-1.el9    centreon-25.10-stable-noarch  3.3 k
 centreon-mariadb  noarch  25.10.3-1.el9    centreon-25.10-stable-noarch  3.4 k
 centreon-web      noarch  25.10.3-1.el9    centreon-25.10-stable-noarch   21 M

Transaction Summary
================================================================================
Upgrade  4 Packages

Total size: 21 M
Is this ok [y/N]:
```

- **Vérification des plugins nécessaires**

Vérification des plugins nécessaires Pour s’assurer de la présence des plugins indispensables au bon fonctionnement de Centreon, il convient de lister les modules disponibles à l’aide de la commande suivante :

```bash
[root@centreon-central-25 ~]# ls /usr/lib/centreon/plugings/
ls: cannot access '/usr/lib/centreon/plugings/': No such file or directory
[root@centreon-central-25 ~]# ls /usr/lib/centreon/plugins
centreon_centreon_central.pl     centreon_printers_generic_snmp.pl
centreon_centreon_database.pl    centreon_protocol_dns.pl
centreon_centreon_map.pl         centreon_protocol_ftp.pl
centreon_centreon_poller.pl      centreon_protocol_http.pl
centreon_cisco_standard_snmp.pl  centreon_protocol_ldap.pl
centreon_linux_snmp.pl           centreon_ups_standard_rfc1628_snmp.pl
centreon_mysql.pl                centreon_windows_snmp.pl
[root@centreon-central-25 ~]#
```

- **Démarrage et activation des services Centreon**

Pour garantir le bon fonctionnement de la plateforme Centreon, il est nécessaire de démarrer et d'activer les services critiques. Les commandes suivantes permettent de lancer les services et de les configurer pour un démarrage automatique à chaque redémarrage du serveur :

```bash
sudo systemctl start centreon
sudo systemctl enable centreon

sudo systemctl start centengine
sudo systemctl enable centengine

sudo systemctl start cbd
sudo systemctl enable cbd

sudo systemctl start gorgoned
sudo systemctl enable gorgoned
```

Cette étape assure que la plateforme Centreon demeure opérationnelle et que les services critiques sont automatiquement relancés à chaque redémarrage du serveur.

2- Configuration SMTP

Cette étape consiste à mettre en place le serveur de messagerie qui servira de relais pour l'envoi des notifications par mail. La configuration inclut :

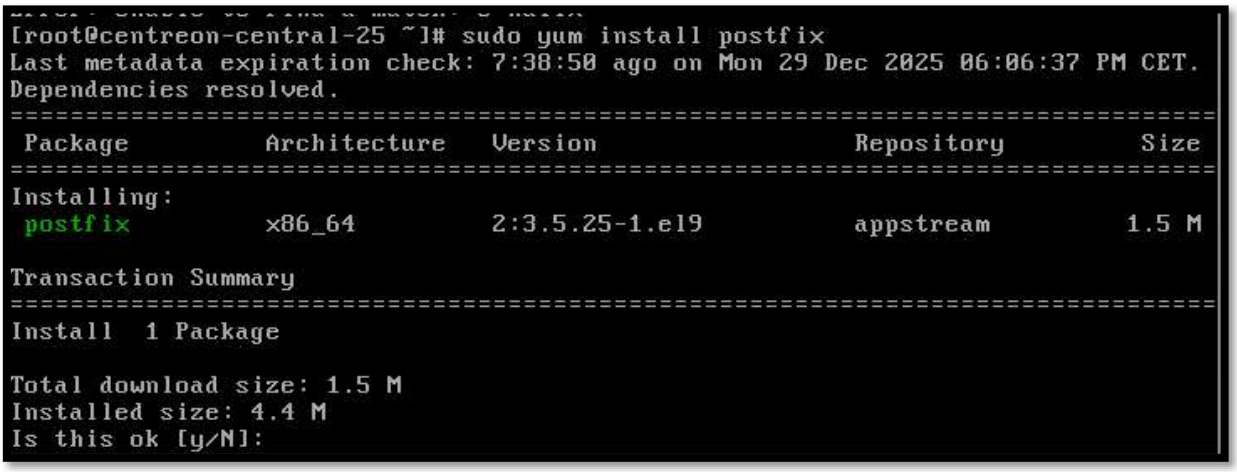
- L'installation des paquets **Postfix** et **s-nail** afin de tester l'envoi et la réception des messages.
- L'installation de l'éditeur de texte ***nano*.** Cet outil léger et convivial permet de modifier les fichiers système directement depuis le terminal.
- L'édition du fichier de configuration `/etc/postfix/main.cf` ainsi que la mise en place de l'authentification **SMTP** pour permettre la réception des mails sur un compte **Gmail**.

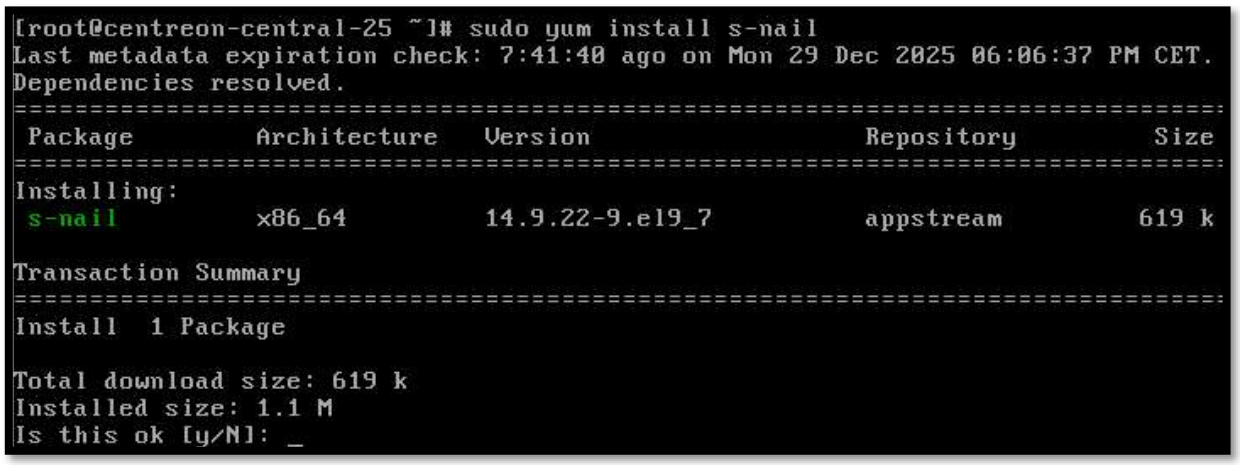
- Installation de Nano

✓ **Installation des paquets**

L'installation des composants nécessaires se fait à l'aide de la commande suivante :

```bash
sudo yum install postfix s-nail
```

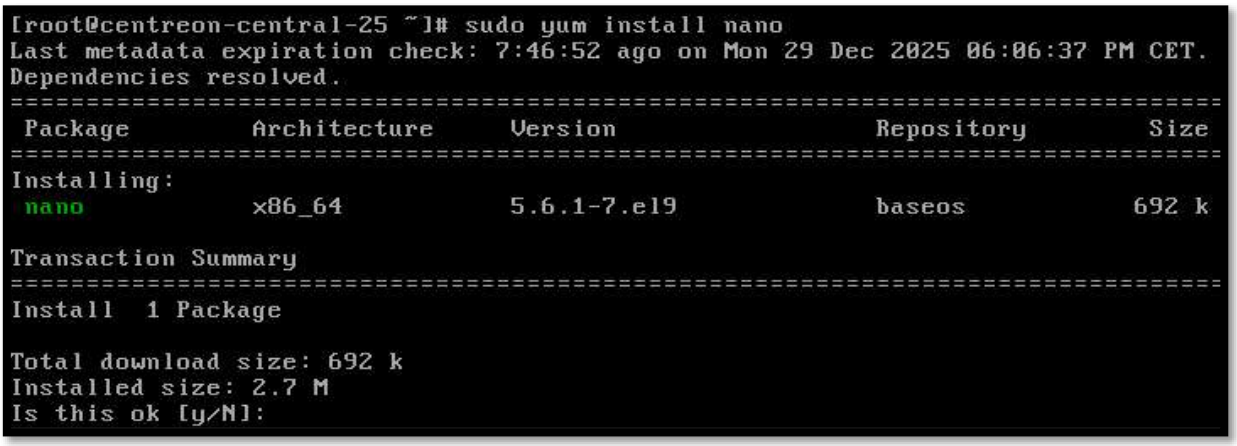




- **Installation de nano**

Afin de faciliter l'édition des fichiers de configuration, nous avons procédé à l'installation de l'éditeur de texte *nano*. Cet outil léger et convivial permet

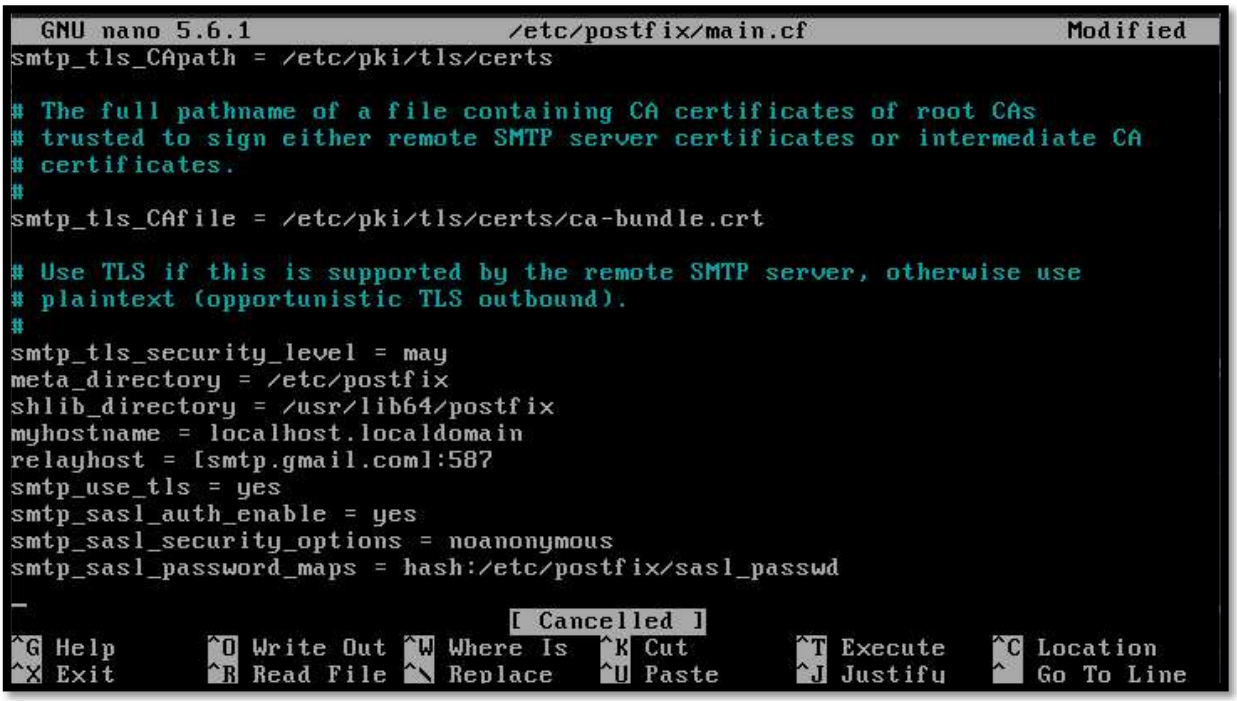
de modifier rapidement les fichiers système directement depuis le terminal.



- **Configuration du fichier /etc/postfix/main.cf**

L'édition du fichier de configuration principal de **Postfix** est nécessaire afin de définir les paramètres du service **SMTP**. Cette opération s'effectue sur le serveur central (**Centreon**) en exécutant la commande suivante :

```
“‘bash”’
sudo nano /etc/postfix/main.cf
```



Ce fichier permet de spécifier les options essentielles du serveur de messagerie, telles que le nom d'hôte, le domaine, le relais SMTP et les règles de sécurité.

- **Configuration de l'authentification SMTP**

Après avoir défini les paramètres principaux dans le fichier de configuration de Postfix, il est nécessaire de mettre en place l'authentification SMTP afin de permettre au serveur d'utiliser un relais de messagerie externe (par

```
“‘bash’’’
sudo nano /etc/postfix/sasl_passwd
```

exemple Gmail). Cette opération s'effectue en éditant le fichier suivant :

Dans ce fichier, on renseigne les informations d'authentification du relais SMTP, telles que l'adresse du serveur, le port utilisé et les identifiants de connexion. Cette étape est indispensable pour sécuriser la communication et garantir l'envoi correct des notifications par mail.

Après avoir renseigné les identifiants dans le fichier /etc/postfix/sasl_passwd, il est indispensable de le sécuriser afin de protéger les informations sensibles. Cette opération s'effectue en exécutant les commandes suivantes :

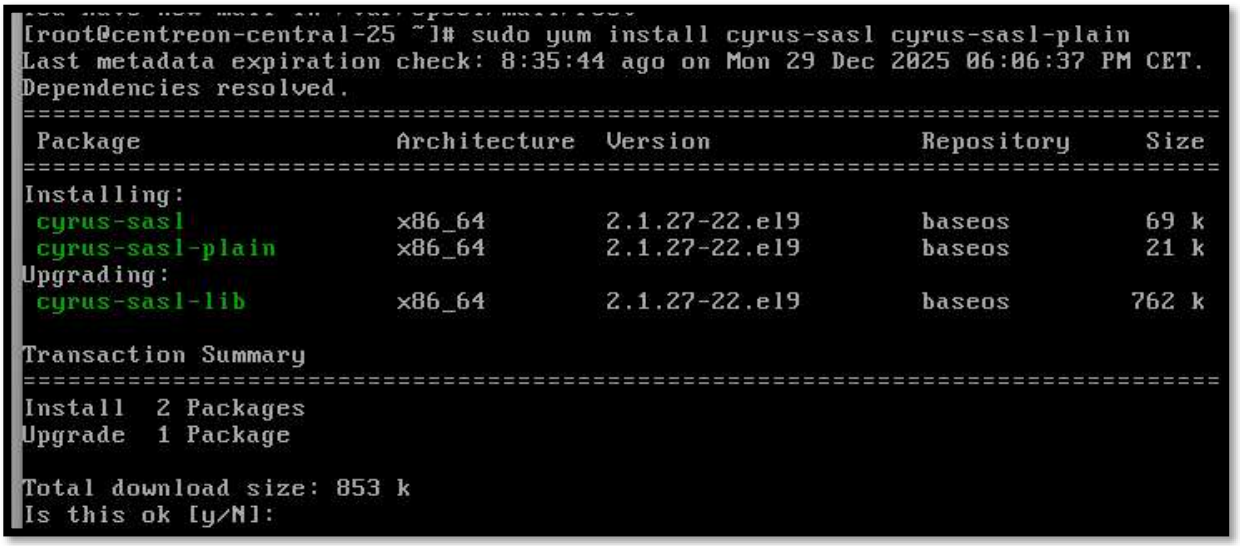
```
“‘bash’’’
sudo postmap /etc/postfix/sasl_passwd
sudo chmod 600 /etc/postfix/sasl_passwd
sudo chmod 600 /etc/postfix/sasl_passwd.db
```

La première commande génère une base de données lisible par **Postfix** à partir du fichier d'authentification, tandis que la seconde restreint les permissions pour que seul l'administrateur (root) puisse accéder au fichier. Ces mesures garantissent la confidentialité des identifiants et renforcent la sécurité du service **SMTP.**

- **Installation des modules d'authentification SASL**

Afin de permettre à Postfix d'utiliser le mécanisme d'authentification requis par Gmail (notamment PLAIN), il est nécessaire d'installer les modules SASL appropriés. Cette étape est indispensable pour que le serveur puisse établir une connexion sécurisée avec le relais SMTP. L'installation s'effectue à l'aide de la commande suivante :

```bash
sudo yum install cyrus-sasl cyrus-sasl-plain -y
```



- **Démarrage et test du service Postfix**

Une fois le fichier d'authentification sécurisé, il est nécessaire d'activer et de démarrer le service Postfix afin d'assurer son bon fonctionnement. Les commandes suivantes permettent de l'activer au démarrage du système, de relancer le service et de vérifier son état :

```bash
sudo systemctl enable postfix
sudo systemctl restart postfix
sudo systemctl status postfix
```

La première commande configure Postfix pour qu'il démarre automatiquement à chaque redémarrage du serveur. La seconde relance le service afin de prendre en compte les modifications de configuration. Enfin, la troisième permet de vérifier que Postfix est bien actif et opérationnel.

Enfin, afin de valider le bon fonctionnement du serveur Postfix et confirmer que l'authentification SMTP est correctement configurée, nous réalisons un test d'envoi de message. La commande suivante permet d'envoyer un mail de test vers une adresse Gmail :

```
“‘bash’’’
echo "Test de Postfix et Vérification de base" | mail -v -s "Centreon" junioragbenonzan31@gmail.com
```

Grâce à l'intégration et à la configuration du service Postfix avec authentification SMTP, Centreon est désormais en mesure d'envoyer automatiquement des notifications par courrier électronique en cas d'incident détecté sur les serveurs ou services supervisés. Cette fonctionnalité garantit une réactivité accrue des administrateurs face aux anomalies et contribue à la fiabilité globale du système de supervision.

3- Configuration SMTP sur le serveur linux

Cette étape constitue le point de départ du processus de supervision. Elle comprend :

- **L'installation du protocole SNMP**, indispensable pour permettre la collecte des informations système.
- **La configuration du service SNMP**, réalisée à travers l'édition du fichier /etc/snmp/snmpd.conf afin d'adapter les paramètres de communication.
- **Un test de communication**, qui permet de vérifier que le service est opérationnel et que le serveur peut être supervisé correctement par la plateforme Centreon.
- **Installation**

Étant connecté au serveur Linux, nous procédons à l'installation du protocole SNMP ainsi que des utilitaires nécessaires. Cette opération

permet d'activer la collecte des informations système indispensables à la supervision. La commande suivante est utilisée :

```bash
sudo apt install snmp snmpd -y
```

Cette commande installe le paquet principal **snmp**, qui fournit le service SNMP, ainsi que **snmpd**, qui contient les outils de gestion et de test (comme snmpwalk et snmpget). L'option -y permet de valider automatiquement l'installation sans demander de confirmation. L'installation du paquet SNMP ayant déjà été effectuée, le système indique que celui-ci est présent. Nous procédons ensuite à la vérification de l'état du service SNMP sur le serveur à l'aide de la commande suivante :

```bash
sudo systemctl status snmpd
```

```
juroot@ubuntuvi:~$ systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
     Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-12-30 02:03:15 UTC; 6min ago
   Main PID: 662 (snmpd)
      Tasks: 1 (limit: 4558)
     Memory: 9.5M
        CPU: 632ms
     CGroup: /system.slice/snmpd.service
             └─662 /usr/sbin/snmpd -LOw -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTrigge>

Warning: some journal files were not opened due to insufficient permissions.
lines 1-11/11 (END)
```

Cette vérification permet de confirmer que le service est bien actif et opérationnel.

La vérification confirme que le service SNMP est bien activé sur notre serveur depuis le **30/12/2025 à 02h03min15s**. Afin de garantir que ce

```
juroot@ubuntuvi:~$ systemctl enable snmpd
Synchronizing state of snmpd.service with SysV service script with /lib/systemd/systemd-sysv-install
.
Executing: /lib/systemd/systemd-sysv-install enable snmpd
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: juroot
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: juroot
Password:
==== AUTHENTICATION COMPLETE ===
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: juroot
Password:
==== AUTHENTICATION COMPLETE ===
juroot@ubuntuvi:~$ _
```

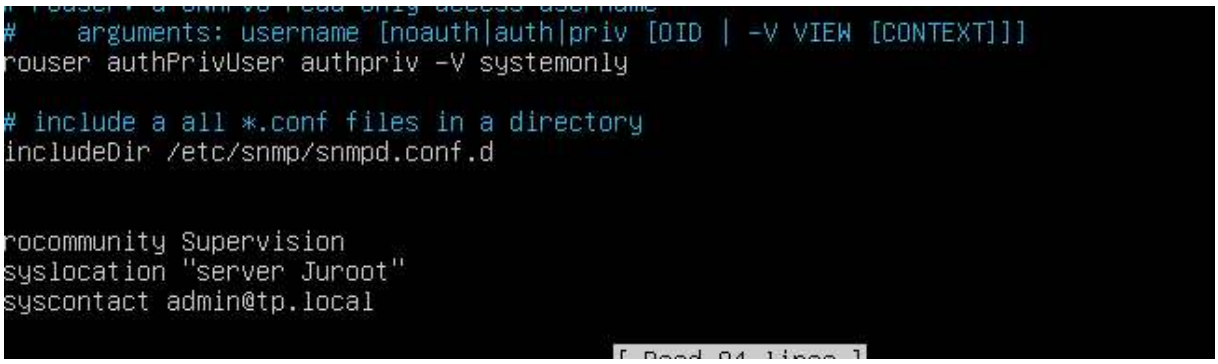
service démarre automatiquement à chaque redémarrage du système, nous exécutons la commande suivante :

```bash
sudo systemctl enable snmpd
```

- **Édition du fichier de configuration SNMP**

Après l'installation et l'activation du service SNMP, il est nécessaire de procéder à sa configuration afin d'adapter les paramètres de supervision. Pour cela, nous éditons le fichier de configuration principal avec la commande suivante :

```bash
sudo nano /etc/snmp/snmpd.conf
```



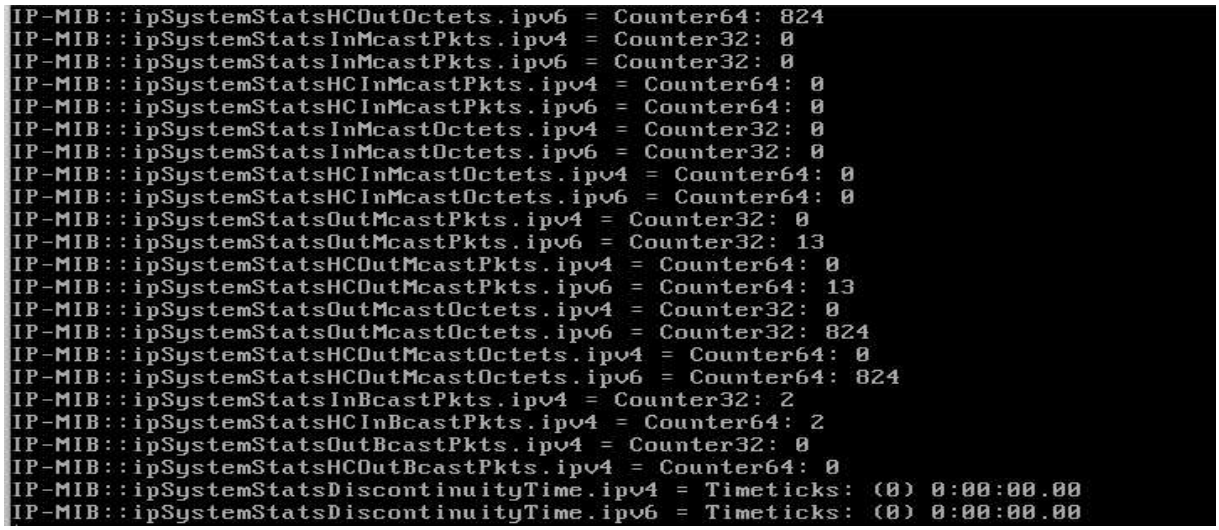
Ce fichier permet de définir la communauté SNMP, les règles d'accès ainsi que les options de communication entre le serveur supervisé et la plateforme Centreon.

- **Test de communication SNMP**

Afin de vérifier le bon fonctionnement du service SNMP, nous réalisons un test de communication depuis le serveur central (Centreon). Ce test permet de s'assurer que l'hôte supervisé répond correctement aux requêtes SNMP. La commande utilisée est la suivante :

```bash
snmpwalk -v2c -c Supervision IP_du_serveur
```

Cette commande interroge l'hôte distant en utilisant le protocole SNMP version 2c et la communauté définie sous le nom **Supervision**. Si la configuration est correcte, le résultat attendu est une liste d'OIDs correspondant aux informations système collectées sur le serveur supervisé.



4- Configuration SNMP sur le serveur Windows 2019

Etant donné que celui-ci sera supervisé en SNMP comme le serveur linux, nous allons

Installer et activer le service SNMP sur ce serveur.

- **Installation du service SNMP sur le serveur Windows**

Il existe deux modes d'installation de ce service : Installation en mode graphique et

Installation en PowerShell. Nous avons opté pour l'installation en mode graphique.

Pour l'activation de ce service, rendons-nous sur notre serveur Windows et suivons les étapes

suivantes :

- ✓ Ouvrez le Gestionnaire de serveur
- ✓ Cliquez sur Ajouter des rôles et des fonctionnalités
- ✓ Sous Avant de commencer, cliquez sur Suivant
- ✓ Sous Sélectionner le type d'installation, cliquez sur Suivant

- ✓ Sous Sélectionner le serveur de destination, cliquez sur Suivant
- ✓ Sous Sélectionner les rôles du serveur, cliquez sur Suivant
- ✓ Sous Sélectionner les fonctionnalités, cochez Service SNMP, puis cliquez sur Ajouter des fonctionnalités, ensuite cliquez sur Suivant
- ✓ Sous Confirmer la sélection d'installation, cliquez sur Installer
- ✓ Attendez que l'installation soit terminée

➢ **Configuration du SNMP service**

- ✓ Pour configurer le SNMP nous allons suivre les étapes suivantes :
- ✓ Ouvrir l'applet Services (cliquez sur le menu Démarrer et recherchez services)
- ✓ Recherchez le service SNMP, faites un clic droit dessus puis cliquez sur Propriétés.
- ✓ Cliquons sur Sécurité, puis sur Ajouter. Ajoutez le nom de la communauté (dans notre cas c'est : public).

Après avoir configurer la communauté, on clique sur :

- ✓ Accepter les paquets SNMP provenant de ces Hôtes
- ✓ Ajouter, Appliquer , puis sur Ok

5- Intégration des hôtes et sevices

a- Création des Hôtes dans Centreon

La création d'un hôte dans Centreon consiste à définir les paramètres nécessaires pour permettre la supervision du serveur Linux via SNMP. Les informations à renseigner sont les suivantes :

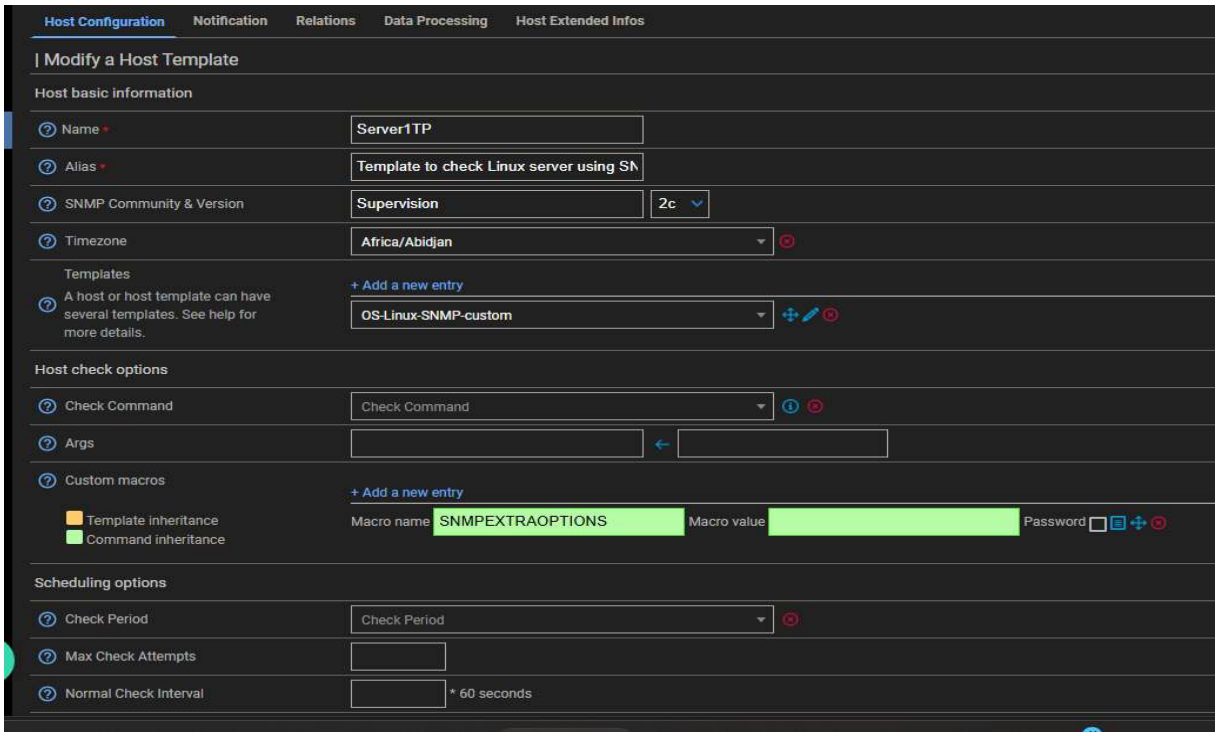
- **Nom de l'hôte** : correspond au nom attribué à notre serveur.
- **Alias ou description** : une brève description permettant d'identifier facilement le serveur.
- **Adresse IP** : l'adresse réseau du serveur supervisé.
- **Communauté SNMP et version** : dans notre cas, la communauté est Supervision et la version utilisée est SNMP v2c.

Ensuite, dans le champ Modèle, nous cliquons sur le bouton + Ajouter une nouvelle entrée et sélectionnons le modèle OS-Linux-SNMP-custom.

Pour ajouter l'hôte, nous naviguons dans le menu :

Configuration > Hôtes > Hôtes > Ajouter, puis nous renseignons les informations ci-dessus.

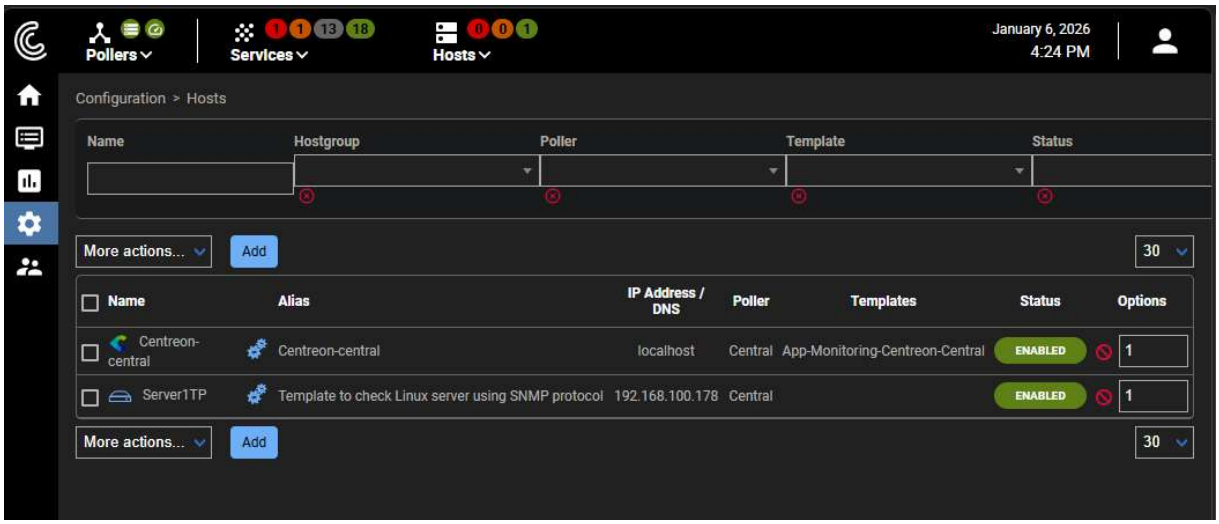
Cette étape permet d'intégrer notre serveur Linux à la plateforme Centreon afin qu'il soit supervisé via SNMP.



De la même manière, nous procédons à l'intégration des autres serveurs ainsi que des applications à notre plateforme de supervision.

Après avoir renseigné les informations nécessaires et cliqué sur Enregistrer, nous constatons que l'ensemble de nos serveurs ont bien été ajoutés à Centreon. Ils apparaissent désormais dans la plateforme et sont tous supervisés via le protocole SNMP.

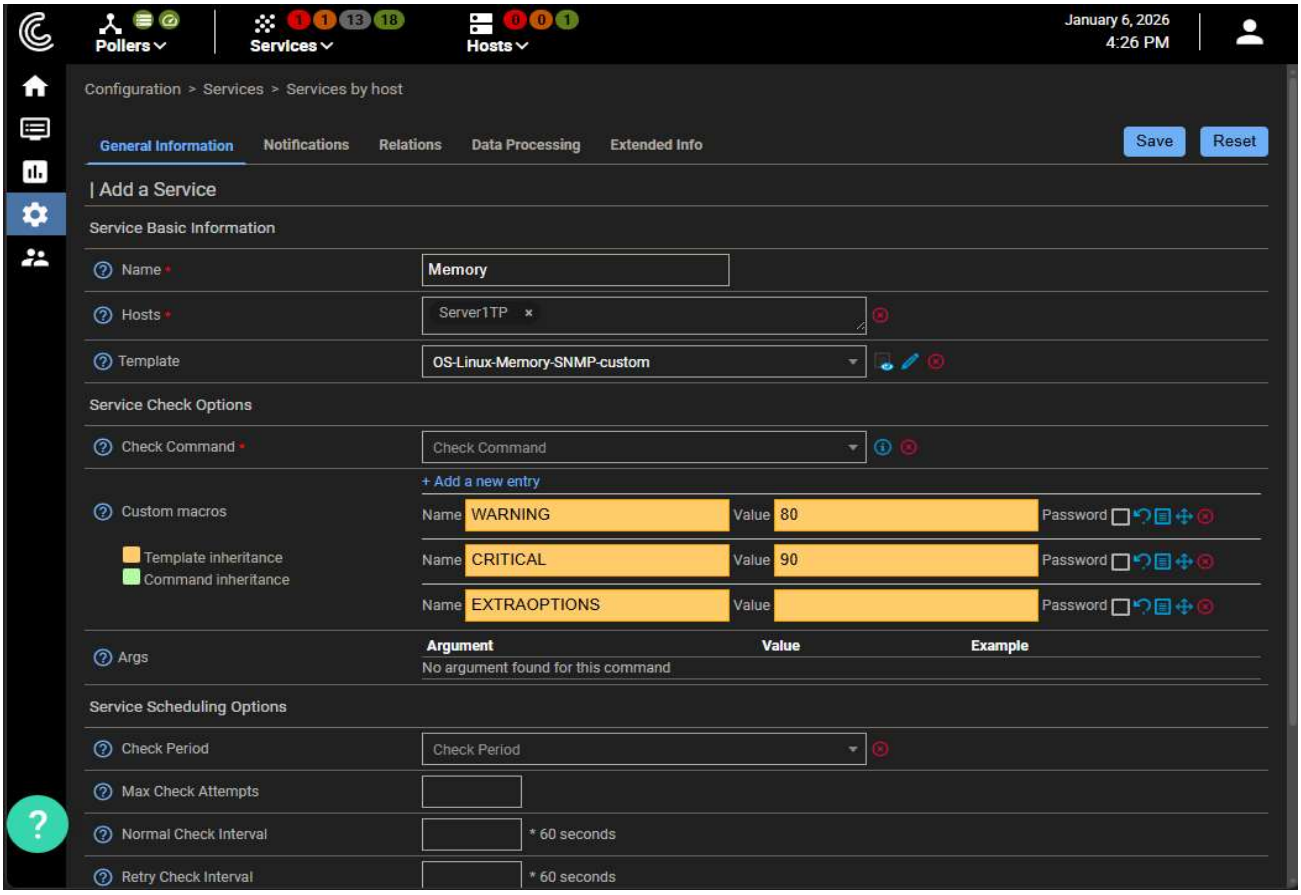
Dans le menu Supervision > Détails des statuts > Regroupement par hôte, une vue synthétique est disponible. Elle permet de visualiser clairement l'ajout de nos différents serveurs et de vérifier leur état de supervision.



b- Création des Services

Après l'ajout des serveurs à la plateforme de supervision, nous passons à l'étape suivante : l'ajout des services associés à chaque hôte. La création d'un service dépend directement de l'hôte auquel il est lié et nécessite de renseigner plusieurs informations :

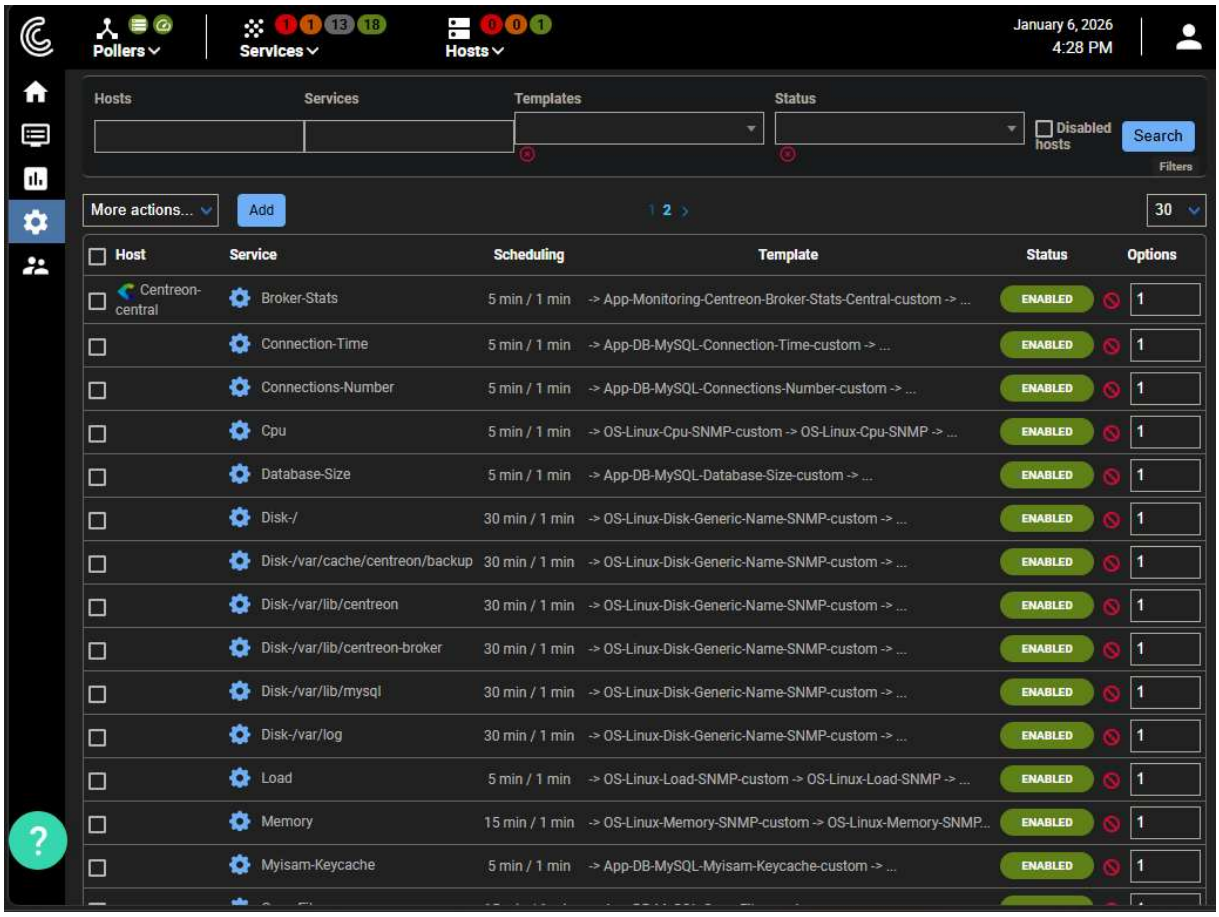
- **Description du service** : par exemple CPU pour la supervision de l'utilisation du processeur.
- **Hôte associé** : le nom du serveur qui héritera de ce service.
- **Modèle :** le modèle de supervision correspondant. Dans le cas d'un serveur Linux supervisé en SNMP, nous utilisons le modèle **OS-Linux-Cpu-SNMP-custom.**



Ainsi cela fait nous naviguons dans le menu :

Configuration > Services > Services par hôte, puis nous cliquons sur Ajouter afin de renseigner les informations propres à chaque service.

Une fois cette étape réalisée, nous obtenons une vue récapitulative listant l'ensemble des services associés à nos hôtes. Cette interface permet de vérifier que tous les indicateurs critiques (CPU, RAM, disque, réseau, etc.) sont bien pris en compte dans la supervision.



c- Configuration des notifications

Les notifications constituent un élément essentiel de la supervision, car elles permettent aux administrateurs d'être alertés en temps réel lorsqu'un problème survient sur un hôte ou un service. Grâce à ces alertes, il est possible de réagir rapidement et de prendre les mesures nécessaires pour rétablir le bon fonctionnement du système.

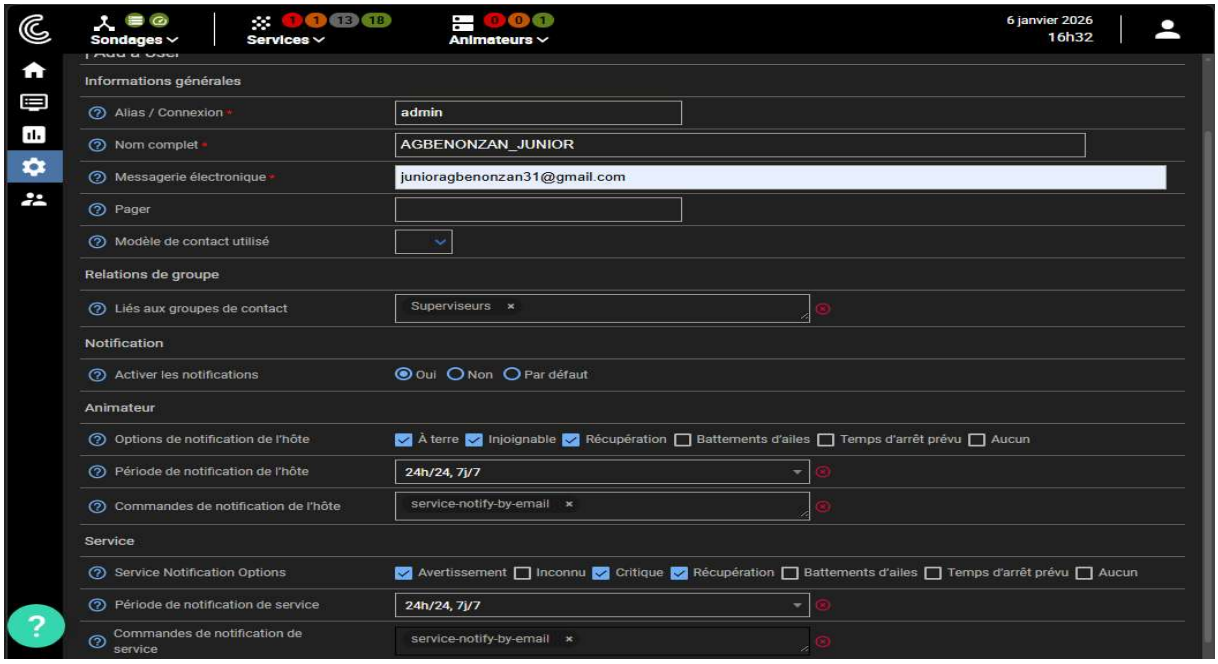
La configuration des notifications dans Centreon implique :

- Activation des notifications pour les hôtes et services critiques.
- Définition des conditions de déclenchement (par exemple : changement d'état vers Warning ou Critical).
- Spécification des destinataires (administrateurs ou équipes responsables).
- Choix du canal de communication (e-mail, SMS, ou scripts personnalisés).

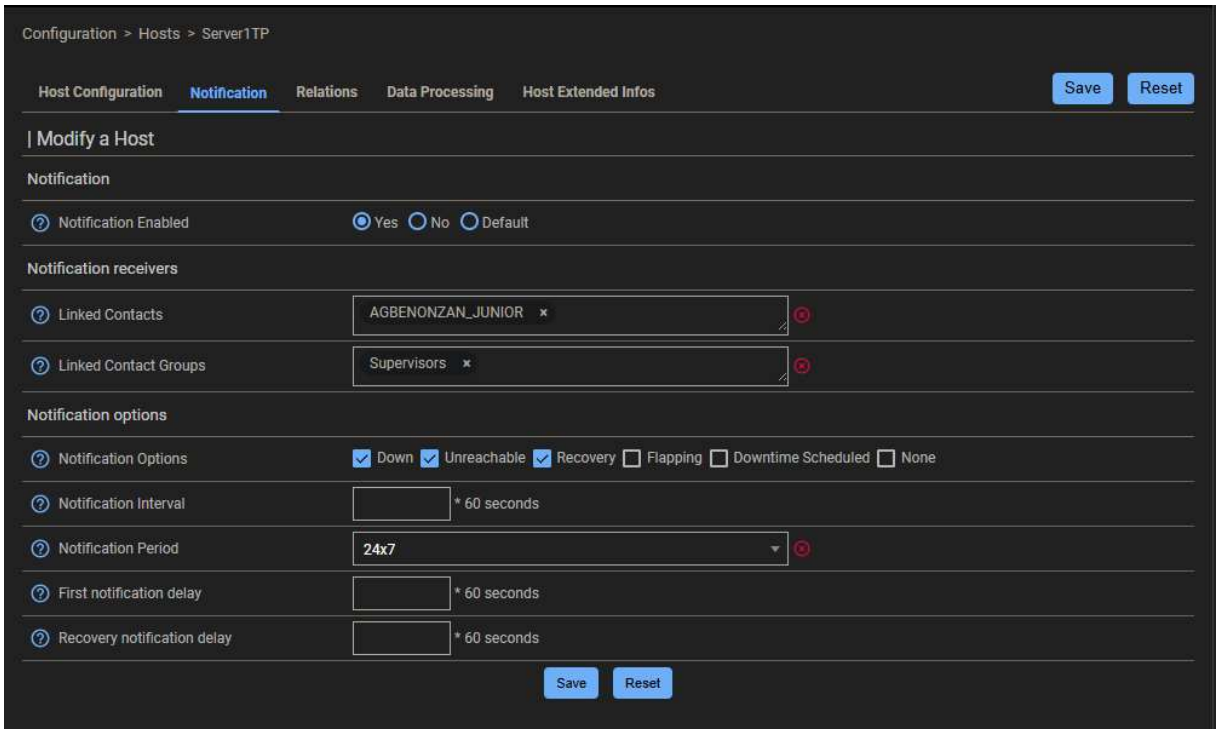
- Association aux hôtes et services concernés, afin que seuls les éléments supervisés et jugés importants génèrent des alertes.

Dans Centreon, cette configuration se fait via le menu :

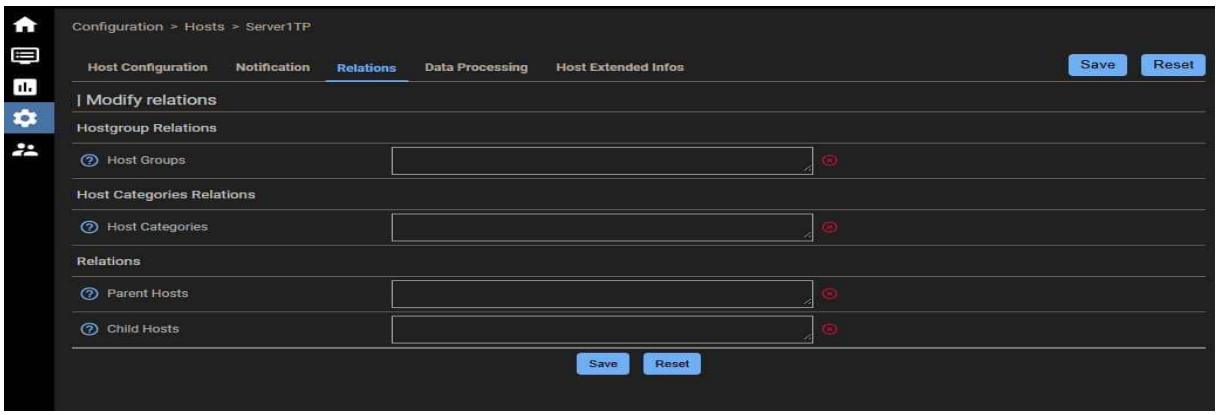
Configuration > Hôtes/Services > Notifications, où l'on peut activer et personnaliser les paramètres selon les besoins de l'organisation.



d- Association des contacts aux hotes



e- Association des services aux hotes



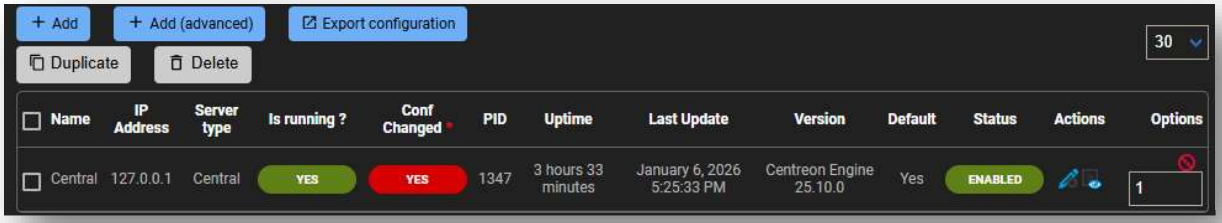
f- Déploiement des configurations

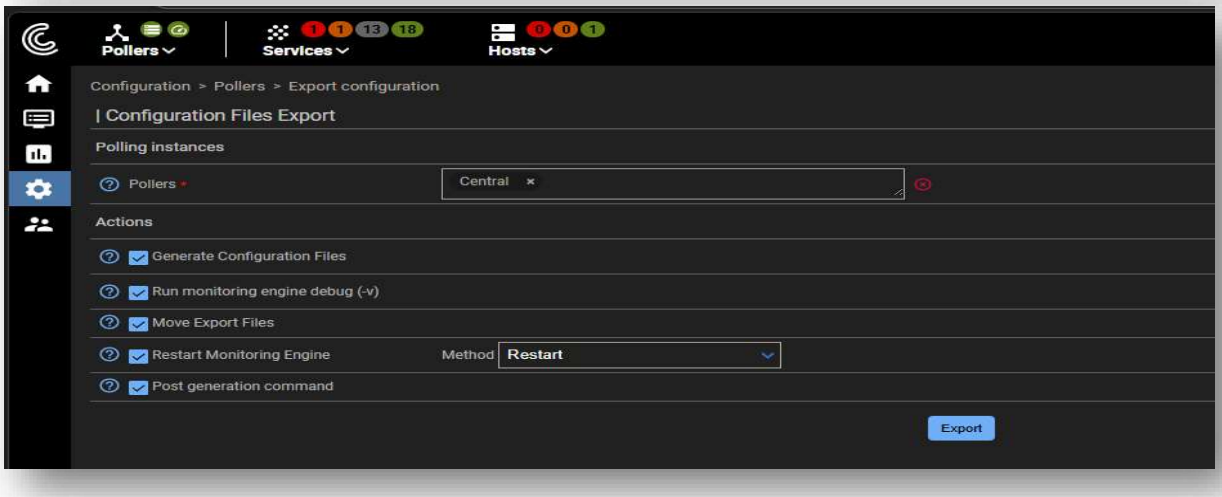
Une fois les hôtes et services créés dans Centreon, il est nécessaire de déployer les configurations afin que le moteur de supervision prenne en compte les nouveaux paramètres. Cette étape se déroule en plusieurs phases :

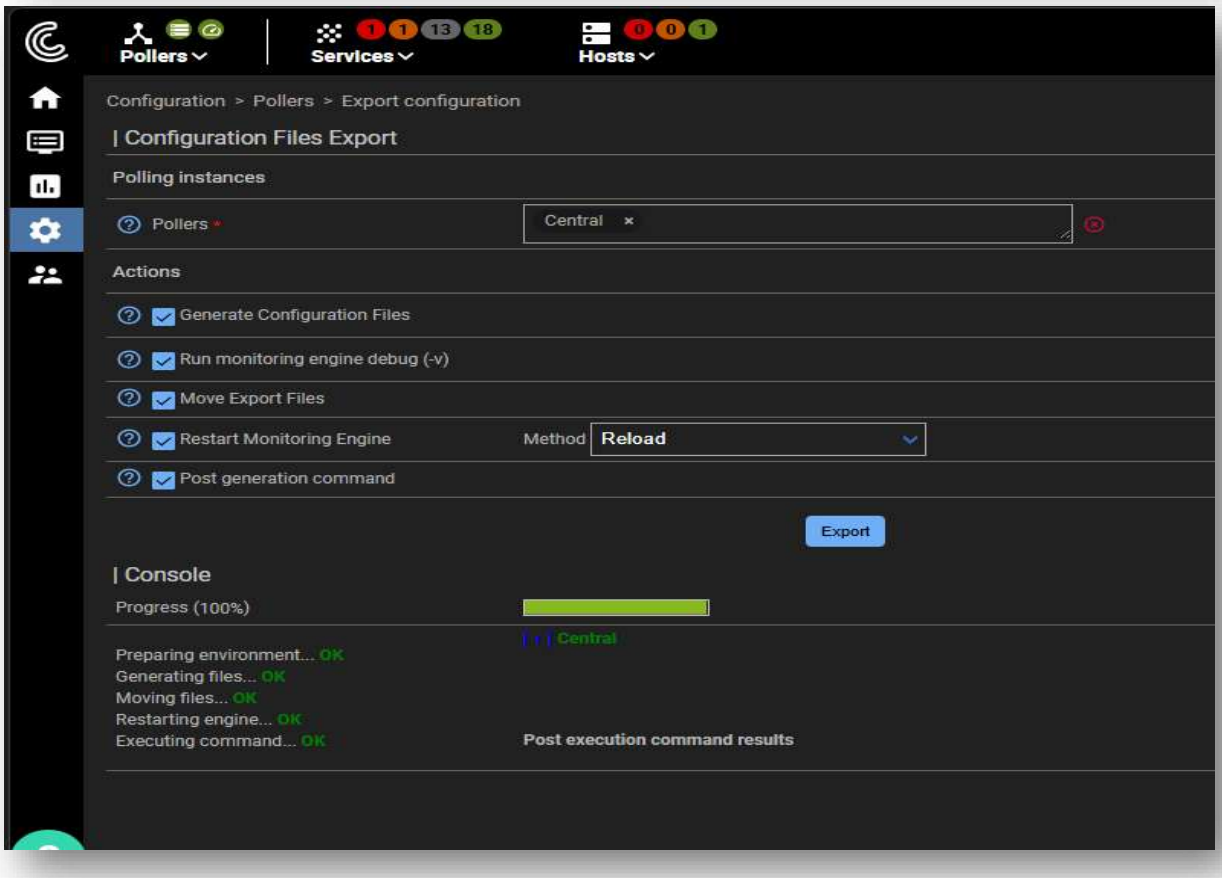
- **Génération des fichiers de configuration** : Centreon compile les informations saisies (hôtes, services, modèles, notifications) pour produire les fichiers nécessaires au moteur de supervision.
- **Lancement du débogage du moteur de supervision** : cette vérification permet de s'assurer qu'aucune erreur n'est présente dans les fichiers générés.

- **Déplacement des fichiers générés :** les fichiers de configuration validés sont transférés vers le répertoire utilisé par le moteur de supervision.
- **Redémarrage de l'ordonnanceur :** cette action recharge les nouvelles configurations et active la supervision des hôtes et services ajoutés.

Cette étape est cruciale, car elle valide et applique l'ensemble des paramètres définis dans l'interface Centreon, garantissant ainsi une supervision opérationnelle et fiable.


+ Add
+ Add (advanced)
Export configuration
Duplicate
Delete
30
Name
IP Address
Server type
Is running ?
Conf Changed
PID
Uptime
Last Update
Version
Default
Status
Actions
Options
Central
127.0.0.1
Central
YES
YES
1347
3 hours 33 minutes
January 6, 2026 5:25:33 PM
Centreon Engine 25.10.0
Yes
ENABLED
1


Pollers
Services
Hosts
Configuration > Pollers > Export configuration
| Configuration Files Export
Polling instances
Pollers *
Central
Actions
Generate Configuration Files
Run monitoring engine debug (-v)
Move Export Files
Restart Monitoring Engine
Method
Restart
Post generation command
Export


Pollers
Services
Hosts
Configuration > Pollers > Export configuration
| Configuration Files Export
Polling instances
Pollers *
Central
Actions
Generate Configuration Files
Run monitoring engine debug (-v)
Move Export Files
Restart Monitoring Engine
Method
Reload
Post generation command
Export
| Console
Progress (100%)
Central
Preparing environment... OK
Generating files... OK
Moving files... OK
Restarting engine... OK
Executing command... OK
Post execution command results

6- Scénarios des test

Dans le cadre de l'implémentation de la solution de supervision Centreon, plusieurs scénarios de tests ont été réalisés afin de valider le bon fonctionnement du système et de garantir la fiabilité de la supervision mise en place.

Les objectifs de ces tests sont les suivants :

- ✓ **Validation de la communication SNMP** : vérifier que les serveurs Linux et Windows supervisés répondent correctement aux requêtes SNMP émises par la plateforme Centreon.
- ✓ **Contrôle de la collecte des métriques :** s'assurer que les indicateurs essentiels (CPU, mémoire, espace disque, services critiques) sont bien collectés et affichés dans l'interface Web Centreon.
- ✓ **Test des alertes automatiques** : confirmer que des alertes sont générées en cas d'anomalie et transmises à l'administrateur via SMTP, grâce à l'intégration avec Gmail.
- ✓ **Vérification des notifications en temps réel** : garantir que les notifications sont effectivement reçues sur le téléphone mobile de l'administrateur, permettant une réactivité immédiate face aux incidents

a- Quelque resultats des tests

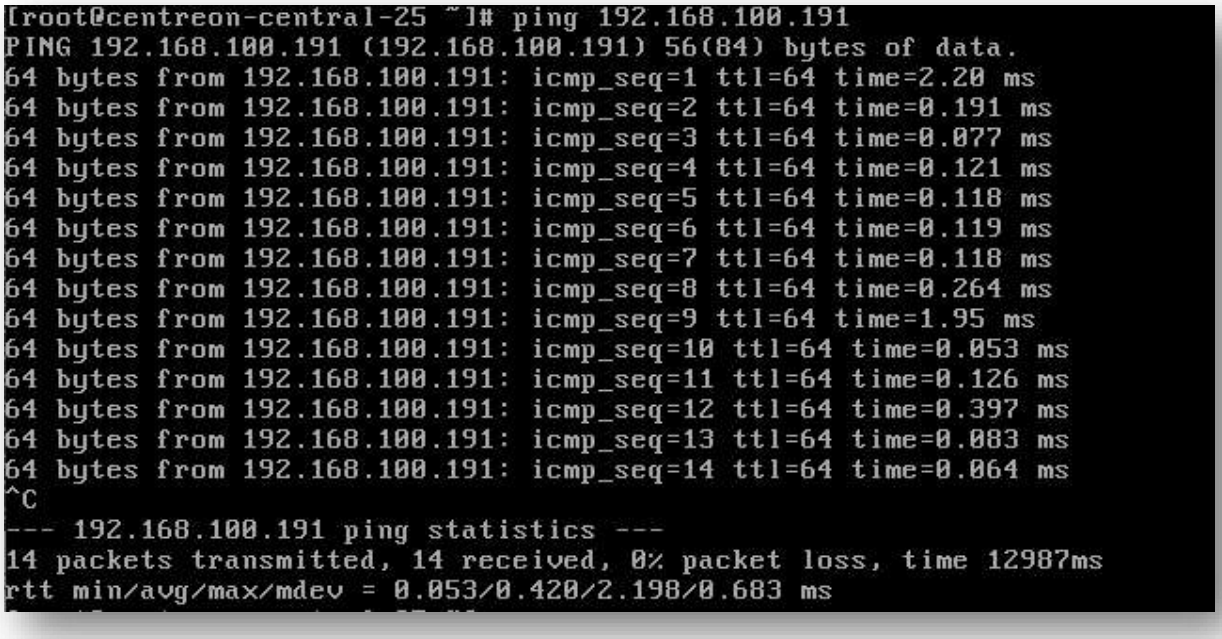
Dans cette partie nous présenterons les résultats de notre scénario de test

- **Test ping entre serveur Windows et serveur Centreon**

```
Microsoft Windows [version 10.0.26220.7523]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Junio>ping 192.168.100.191

Envoi d'une requête 'Ping'  192.168.100.191 avec 32 octets de données :
Réponse de 192.168.100.191 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.191 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.191 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.100.191 : octets=32 temps=3 ms TTL=64

Statistiques Ping pour 192.168.100.191:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms

C:\Users\Junio>
```

D’après les statistiques du ping vers IP du serveur Centreon, nous remarquons aussi qu’il y a eu 4 paquets transmis au serveur central par le serveur Windows, dont 4 reçu avec succès et zéro perdu en 2ms soit 3/1000 s. On peut conclure que la transmission de données du serveur Windows au serveur Centreon est parfaite. Donc la réciprocité de communication entre ces deux serveurs est vérifiée

- **Test Ping entre server linux et serveur centreon**



Conclusion

La mise en œuvre de la solution de supervision avec **Centreon** dans un environnement virtualisé sous **VMware Workstation Pro** démontre la puissance d'une approche centralisée pour garantir la disponibilité et la performance des infrastructures informatiques. Grâce à l'intégration des serveurs Linux, Windows et Apache, la configuration des hôtes et services, ainsi que l'activation des notifications, nous avons construit un système capable de détecter, analyser et signaler en temps réel toute anomalie critique.

Ce projet illustre non seulement la maîtrise des concepts de **virtualisation et de supervision réseau**, mais aussi leur importance stratégique dans la gestion moderne des systèmes d'information. La supervision devient ainsi un véritable levier de **sécurité, fiabilité et proactivité**, permettant aux administrateurs d'anticiper les incidents et d'assurer une continuité de service optimale.

En définitive, cette expérience pratique prouve que la combinaison de **Centreon et SNMP** constitue une solution robuste et évolutive, capable de répondre aux exigences des environnements professionnels. Elle ouvre la voie à une gestion intelligente des infrastructures, où chaque ressource est surveillée, chaque alerte est maîtrisée, et chaque décision est éclairée par une visibilité complète sur le système.